Sumário

Siglas e Definições

Termos e acrônimos comuns que podem ser usados ao longo deste documento.

CGPSI	Comitê Gestor de Política de Segurança da Informação.
CGSI	Comitê Gestor de Segurança da Informação.
Criptografia	O processo de transformar informações, usando um algoritmo, para torná-las ilegíveis para qualquer pessoa, exceto aqueles que têm uma "necessidade de saber" específica.
Mídia externa	CD-ROMs, DVDs, disquetes, unidades flash, chaves USB, pen drives, fitas.
Firewall	Um hardware ou software dedicado executado em um computador que permite ou nega a passagem de tráfego por ele, com base em um conjunto de regras.
FTP	Protocolo de Transferência de Arquivos
TI	Tecnologia da Informação
LAN	Local Area Network - uma rede de computadores que cobre uma pequena área geográfica, ou seja, um grupo de edifícios, um escritório.
PSI	Política de Segurança da Informação
Usuário	Qualquer pessoa autorizada a acessar um recurso de informação.
Usuários privilegiados	Administradores de sistema e outros especificamente identificados e autorizados pelo gerenciamento de prática.
VLAN	Rede Local Virtual - Uma rede lógica, normalmente criada dentro de um dispositivo de rede, geralmente usada para segmentar o tráfego da rede para fins administrativos, de desempenho e / ou segurança.
VPN	Rede privada virtual - fornece uma passagem segura pela Internet pública.
WAN	Wide Area Network - Uma rede de computadores que permite a comunicação em uma ampla área, ou seja, regional, nacional.
Vírus	Um programa de software capaz de se reproduzir e geralmente capaz de causar grandes danos a arquivos ou outros programas no computador que ele ataca. Um verdadeiro vírus não pode se espalhar para outro computador sem assistência humana.

1. Introdução

"A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário" (Rezende e Abreu, 2000), possui um valor altamente significativo e pode representar grande poder para quem a detém, pois, além de conter valor, está integrada com os processos, pessoas e tecnologias. Diante da sua importância para as tomadas de decisões, as empresas têm-se empenhado em utilizar mecanismos de segurança no sentido de salvaguardar essas informações.

1.1. O Hospital Nossa Senhora das Dores-HNSD e Pronto Socorro Municipal de Itabira-PSMI tem como missão Valorizar a vida e cuidar das pessoas;

1.2. O Hospital Nossa Senhora das Dores-HNSD e Pronto Socorro Municipal de Itabira-PSMI entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados aos seus clientes;

1.3. O Hospital Nossa Senhora das Dores-HNSD e Pronto Socorro Municipal de Itabira-PSMI compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.4. Dessa forma, o Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira, estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. Objetivo

A Política de Segurança da Informação do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira - PSI/HNSD/PSMI visa preservar a confiabilidade, integridade e disponibilidade das informações para a resolução de problemas e tomada de decisão, primando por melhorar a qualidade do atendimento e tratamento do paciente. A PSI/HNSD/PSMI é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores no que diz respeito a seus direitos e responsabilidades com os recursos computacionais da instituição e as informações neles armazenados. Seu propósito é estabelecer as diretrizes a serem seguidas pela instituição no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

Os requisitos e restrições da política definidos neste documento devem se aplicar a infraestruturas de rede, bancos de dados, mídia externa, criptografia, relatórios impressos, filmes, slides, modelos, wireless, telecomunicações, conversas e quaisquer outros métodos usados para transmitir conhecimentos e ideias em todo o hardware, software e mecanismos de transmissão de dados. Esta política deve ser cumprida por todos os colaboradores, ou trabalhadores temporários, contratados e prestadores de serviços.

3. Aplicação

Este documento define os requisitos de segurança comuns para todo os colaboradores e sistemas que criam, mantêm, armazenam, acessam, processam ou transmitem informações. Esta política também se aplica a recursos de informação de propriedade de terceiros, tais como contratantes, entidades do setor privado, nos casos em que a instituição tenha o dever legal, contratual ou fiduciário de proteger tais recursos enquanto estiver sob sua custódia. Em caso de conflito, aplicam-se as medidas mais restritivas. Esta política cobre a infraestrutura de rede que é composto por vários hardwares, softwares, equipamentos de comunicação e outros dispositivos projetados para auxiliar na criação, recebimento, armazenamento, processamento e transmissão de informações. Esta definição inclui equipamentos conectados a qualquer domínio ou VLAN, com ou sem fio, e inclui todos os equipamentos autônomos que são implantados na instituição ou em locais remotos.

4. Diretrizes

4.1. O objetivo da gestão de Segurança da Informação do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

4.2. A Provedoria, Diretoria e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação no Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da empresa.

4.3. É política do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira:

4.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

4.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes.

4.3.3. Garantir a educação e conscientização sobre as práticas adotadas pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira em segurança da informação para Empregados, terceiros contratados e, onde pertinente, clientes.

4.3.4. Atender integralmente requisitos de segurança da informaç aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

4.3.5. Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

4.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria constante de planos de continuidade e recuperação de desastres;

4.3.7. Avaliar periodicamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5. PAPEIS E RESPONSABILIDADE

5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI

5.1.1 Fica constituído o **Comitê Gestor De Segurança Da Informação**, contando com a participação de, pelo menos, um representante da Diretoria Executiva e um membro das seguintes áreas: Tecnologia da Informação, Recursos Humanos, Jurídico, Marketing/Comunicação, Gestão da Qualidade.

5.1.2 É responsabilidade do CGSI:

5.1.2.1 Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

5.1.2.2 Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

5.1.2.3 Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

5.1.2.4 Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira.

5.2. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

5.2.1 É responsabilidade da Gerência de Segurança da Informação:

5.2.1.1 Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

5.2.1.2 Apoiar o CGSI em suas deliberações;

5.2.1.3 Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSI;

5.2.1.4 Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

5.2.1.5 Tomar as ações cabíveis para se fazer cumprir os termos desta política;

5.2.1.6 Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.3. GESTORES DA INFORMAÇÃO

5.3.1 É responsabilidade dos Gestores da Informação:

5.1.1.3 Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;

5.2.1.3 Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;

5.3.1.3 Periodicamente, revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;

5.4.1.3 Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.5.1.3 Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira.

5.4. USUÁRIOS DA INFORMAÇÃO

5.4.1 É responsabilidade dos Usuários da Informação:

5.4.1.1 Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

5.4.1.2 Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

5.4.1.3 Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;

5.4.1.4 Assinar o Termo de Uso de Sistemas de Informação do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

5.4.1.5 Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições informar parágrafo 7

5.5. DIRETORIA EXECUTIVA

5.5.1 Em relação a segurança da informação, cabe a Diretoria Executiva:

5.5.1.1 Aprovar a Política de Segurança da Informação e suas revisões;

5.5.1.2 Aprovar a nomeação dos “proprietários” da informação;

5.5.1.3 Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo CGPSI/HNSD/PSMI.

6. DIRETRIZES GERAIS DA SEGURANÇA DA INFORMAÇÃO.

6.1. TERMO DE USO DOS SISTEMAS INTERNOS

É um documento que estabelece as regras, responsabilidades e restrições para a utilização dos sistemas, redes e ativos de informação de uma organização. Ele define diretrizes para acesso, confidencialidade, uso adequado dos recursos tecnológicos e sanções em caso de descumprimento. Seu objetivo é garantir a segurança da informação, a conformidade com regulamentações e a proteção contra acessos indevidos ou mau uso. O termo deve ser aceito por todos os usuários antes de utilizarem os sistemas institucionais.

6.2. ACESSO REMOTO

6.2.1. DIRETRIZES GERAIS DE ACESSO REMOTO

- O acesso remoto aos ativos, serviços de informação e recursos computacionais do HNSD e PSMI é **restrito exclusivamente a usuários autorizados** que necessitem desse recurso para o desempenho de suas atividades profissionais.
- O acesso remoto realizado **fora do expediente normal de trabalho** não implicará em pagamento de horas extras, **exceto** nos casos em que houver solicitação formal do gestor do usuário ou de uma parte devidamente autorizada.
- O usuário será **integralmente responsável** por todas as ações realizadas com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada conduzida por terceiros que tenham obtido, de forma lícita ou ilícita, suas credenciais.
- O acesso remoto será concedido com os **privilégios mínimos necessários** para a execução das atividades laborais do usuário, respeitando os princípios de segurança da informação e controle de acesso.
- Todos os equipamentos computacionais utilizados para acesso remoto devem:
  - ⇒ Possuir **ferramentas atualizadas de proteção contra códigos maliciosos**, conforme as diretrizes de segurança do HNSD e PSMI.
  - ⇒ Ter um **firewall local ativo** e devidamente configurado para garantir a proteção do ambiente digital.
- Em casos de **acesso não autorizado, extravio, furto ou roubo** de dispositivos computacionais com credenciais de acesso remoto ativas, o usuário responsável deverá **notificar imediatamente a equipe de segurança da informação** para adoção das medidas cabíveis.

6.2.2. CONCESSÃO E USO DE ACESSO REMOTO PARA TERCEIROS

- O acesso remoto aos ativos, serviços de informação e recursos computacionais do HNSD e PSMI poderá ser concedido a terceiros e prestadores de serviço, somente quando estritamente necessário para a execução de suas atividades.
- Para a concessão desse acesso, devem ser observadas as seguintes diretrizes:
  - ⇒ **Acordo de Confidencialidade**: O acesso remoto só será permitido após a formalização de um acordo de confidencialidade entre as partes envolvidas.
  - ⇒ **Duração Limitada:** O acesso será concedido apenas pelo tempo estritamente necessário, sendo limitado a um período máximo de 30 (trinta) dias corridos por concessão.
  - ⇒ **Responsabilidade:** O usuário terceiro e a empresa contratante serão totalmente responsáveis por qualquer ação realizada com as credenciais de acesso fornecidas. Isso inclui qualquer uso indevido por parte de terceiros.
  - ⇒ **Privilégios Mínimos:** O acesso remoto de terceiros será configurado de acordo com os privilégios mínimos necessários, evitando acessos indevidos ou riscos desnecessários.
  - ⇒ **Segurança dos Equipamentos:** Os dispositivos utilizados para acesso remoto devem seguir as mesmas diretrizes aplicáveis aos usuários internos, incluindo proteção contra códigos maliciosos e firewall local ativo.
  - ⇒ Em caso de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros com acesso remoto ativo, a equipe de segurança da informação deverá ser notificada imediatamente.

6.2.3. MONITORAMENTO DO ACESSO REMOTO

- Toda a informação acessada, transmitida, recebida ou produzida por meio do acesso remoto aos ativos e serviços do HNSD e PSMI está sujeita a monitoramento, não havendo qualquer expectativa de privacidade por parte do usuário.
- O HNSD e PSMI se reservam o direito de monitorar, interceptar, registrar, gravar, copiar e divulgar qualquer dado trafegado, sem necessidade de notificação prévia ao usuário, para fins de auditoria, segurança, investigações internas ou determinações legais.
- O monitoramento poderá ser realizado sobre qualquer comunicação originada ou destinada à rede institucional, visando garantir a integridade, segurança e conformidade com as diretrizes da organização.

6.3. USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS

- O Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;
- A seu critério exclusivo, o Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;
- A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da diretoria do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política Geral de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções e punições previstas neste instrumento;
- O Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;
- O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com o Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:

- O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;
- Dispositivos de computação pessoal possuem ferramenta para prevenção de códigos maliciosos e garantem que as assinaturas de códigos maliciosos vão ser atualizadas em tempo real e executam varreduras diariamente;
- Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.

6.4. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

6.4.1. FERRAMENTA DE PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

- O Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;
- Apenas a ferramenta disponibilizada pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira deve ser utilizada na proteção contra códigos maliciosos;
- A ferramenta de proteção contra códigos maliciosos do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira adota as seguintes regras de uso:
- Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;
- As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;
- As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;
- As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;
- Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;

- Caso uma estação de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, ela deverá ser imediatamente isolada da rede corporativa do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira e de qualquer comunicação com a internet;
- Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento dele da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

6.4.2. PREVENÇÃO DOS USUÁRIOS CONTRA CÓDIGOS MALICIOSOS

- Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;
- Os usuários do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira devem seguir as seguintes regras para proteção contra códigos maliciosos:
- Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
- Reportar imediatamente a área de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;
- Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
- Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
- Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.

6.5. USO DE EMAIL E COMUNICADORES INTERNOS

6.5.1. EMAIL

- O Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;
- Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- Quando o usuário fizer uso do serviço institucional, não é permitido:
  - ⇒ Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
  - ⇒ Utilizar de termos ou palavras de baixo calão na redação de mensagens;
  - ⇒ Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do Hospital Nossa Senhora das Dores, excetuando-se quando expressamente autorizados;
  - ⇒ Inscrever o endereço de e-mail do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;
  - ⇒ Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;
  - ⇒ Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;
  - ⇒ Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;
  - ⇒ Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
  - ⇒ Usar o serviço de e-mail para o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

- O serviço de e-mail é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;
- O monitoramento do tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;
- Durante o monitoramento se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail;
- Os usuários do serviço de e-mail devem adotar a assinatura padrão, formatada de acordo com o seguinte modelo:
  - ⇒ Nome Completo
  - ⇒ Setor
  - ⇒ Cargo
  - ⇒ Telefone
- Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:
- “Esta mensagem, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar, copiar o seu conteúdo.”

6.5.2. SERVIÇO DE COMUNICADORES INSTANTÂNEOS

- O serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;
- Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não seja o oficialmente fornecido;
- Quando o usuário fizer uso do serviço de comunicadores instantâneos não é permitido:
  - ⇒ Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de interesse do Hospital;
  - ⇒ Utilizar de termos ou palavras de baixo calão na redação de mensagens;

⇒ Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para pessoas ou entidades que não fazem parte do domínio corporativo do Hospital, excetuando-se quando expressamente autorizados;

⇒ Fazer uso de qualquer técnica forja ou simulação de falsa identidade. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;

⇒ A interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

⇒ A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (SPAM) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de comunicadores instantâneos;

⇒ Usar o serviço de comunicadores instantâneos para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

- O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, não sendo permitido o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;
- O serviço de comunicadores instantâneos do Hospital é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;
- O monitoramento do serviço de comunicadores instantâneos do Hospital tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;
- Durante o monitoramento o Hospital se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de comunicadores instantâneos.

6.6. ACESSO A ATIVOS E SISTEMAS DE INFORMAÇÃO

6.6.1. USUÁRIO / SENHA:

- O Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira fornecem a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;
- As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;
- Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.
- Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:
- Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
- Informar imediatamente a equipe de segurança caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;
- Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;
- Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

6.6.2. SENHA DE ACESSO

- As senhas associadas às contas de acesso pessoal a ativos/serviços de informação ou recursos computacionais são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;
- Nos setores Recepção, Ambulatório, Pronto Atendimento, Faturamento, Clínicas, Controladoria, Farmácia e Postos de Enfermagem existe um usuário por setor com permissão limitada no sistema operacional, para os sistemas gerais cada usuário possui seu login pessoal.
- A instituição adota os seguintes padrões para a geração de senhas de acesso aos seus ativos, serviços de informação e recursos computacionais:
  - ⇒ A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;
  - ⇒ As senhas possuem validade de 180 (cento e oitenta) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;
  - ⇒ As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
  - ⇒ As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
  - ⇒ Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo por, no mínimo, 30 (trinta) minutos;
  - ⇒ Os sistemas de informação manterão um histórico das últimas 03 (três) senhas utilizadas, não permitindo sua reutilização;
  - ⇒ Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da equipe de tecnologia da informação.
  - ⇒ Senhas temporárias são criadas obrigatoriamente com a opção **"O usuário deve alterar a senha no próximo logon"** habilitada e informada ao colaborador/usuário via telefone e/ou e-mail;
  - ⇒ Quando gerar a nova senha, os usuários devem estar atentos as seguintes recomendações:

⇒ Não utilizar nenhuma parte de sua credencial na composição da senha;

⇒ Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

⇒ Não utilizar repetição ou sequência de caracteres, números ou letras;

⇒ Qualquer parte ou variação do nome Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;

⇒ Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

6.6.3. AUTORIZAÇÃO DE ACESSO (Privilégios de acesso)

- A autorização e o nível permitido de acesso ativos/serviços de informação da Hospital é feita com base em perfis que definem o nível de privilégio dos usuários.
- O acesso à ativos/serviços de informação é fornecido a critério do Hospital, que define permissões baseadas nas necessidades laborais dos usuários;
- Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas a equipe de tecnologia da informação.
- Os usuários devem ainda observar as seguintes diretrizes:
  - ⇒ A seu critério exclusivo, o Hospital poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação justificada ao departamento de tecnologia da informação;
  - ⇒ É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse do Hospital tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);
  - ⇒ Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) do Hospital.

6.7. ACESSO A INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS

6.7.1. ACESSO A INTERNET

- O acesso à internet é disponibilizado exclusivamente para usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais.
- Esse acesso pode ser fornecido tanto por meio da rede corporativa interna, quanto por serviços de internet móvel contratados por terceiros.
- Todas as informações acessadas, transmitidas, recebidas ou produzidas através do acesso à internet estão sujeitas a monitoramento, sem qualquer expectativa de privacidade por parte dos usuários.
- A instituição se reserva o direito de, sem aviso prévio, interceptar, registrar, ler, copiar e divulgar informações para pessoas autorizadas, incluindo investigações internas e criminais, garantindo a segurança dos ativos institucionais.

6.7.2. RETRIÇÕES DE USO DA INTERNET

- Durante o uso da internet institucional, não será permitido o acesso, armazenamento ou compartilhamento de conteúdos relacionados a:
  - ⇒ Exploração sexual, pornografia e conteúdo adulto.
  - ⇒ Assédio, ameaças, chantagem ou difamação.
  - ⇒ Discurso de ódio, discriminação ou preconceito com base em qualquer fator social, racial, religioso ou de gênero.
  - ⇒ Promoção ou incentivo ao consumo de álcool, tabaco ou substâncias ilícitas.
  - ⇒ Atos ilícitos, incentivo ao crime ou contravenções penais.
  - ⇒ Propaganda política, seja nacional ou internacional.
  - ⇒ Atividades comerciais desleais ou concorrência desleal.
  - ⇒ Violação de propriedade intelectual ou industrial da instituição.
  - ⇒ Disseminação de códigos maliciosos, vírus ou outras ameaças virtuais.
  - ⇒ Tentativas de comprometer a infraestrutura computacional da organização.
  - ⇒ Divulgação não autorizada de informações classificadas como confidenciais ou de uso interno.
  - ⇒ Uso de sites ou serviços que visem contornar controles de acesso à internet.

6.7.3. USO DE MÍDIAS SOCIAIS E IDENTIDADE CORPORATIVA

- A publicação de qualquer conteúdo institucional em mídias e redes sociais é restrita a setores e usuários autorizados, sendo vedado a demais usuários representar a organização sem autorização expressa.
- No uso de mídias sociais particulares, empregados, prestadores de serviço e terceiros contratados devem seguir as seguintes diretrizes:
  - ⇒ Não utilizar a logomarca, identidade visual ou nome da instituição sem autorização prévia.
  - ⇒ Não criar, interagir ou participar de grupos, páginas ou perfis que empreguem a marca da organização, exceto os canais oficiais.
  - ⇒ Não publicar conteúdos ou comentários relacionados à instituição, seus colaboradores ou parceiros.
  - ⇒ Registros de eventos internos só são permitidos se não comprometerem a imagem da organização e respeitarem a privacidade de pacientes, acompanhantes e áreas restritas.
  - ⇒ É proibida a divulgação de imagens, vídeos ou áudios do ambiente corporativo, salvo autorização expressa ou uso oficial em canais institucionais.

6.8. MONITORAMENTO DE ATIVOS E SEGURANÇA DA INFORMAÇÃO

6.8.1. ABRANGENCIA

- Aplica-se a todos os ativos de TI, serviços de informação e recursos computacionais da organização, incluindo:
  - ⇒ Servidores, estações de trabalho e dispositivos móveis corporativos.
  - ⇒ Redes corporativas e conexões de internet.
  - ⇒ Sistemas internos, aplicativos e serviços em nuvem.
  - ⇒ Armazenamento de dados e backups.
  - ⇒ Correio eletrônico e sistemas de comunicação corporativos.
  - ⇒ Acessos remotos e atividades executadas por usuários internos e terceiros.
- Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros com acesso aos ativos institucionais.

6.8.2. DIRETRIZES GERAIS

- Princípios do Monitoramento:
  - ⇒ O monitoramento deve ser realizado de forma transparente, contínua e alinhada às normativas legais.
  - ⇒ O objetivo é detectar, prevenir e mitigar riscos relacionados à segurança da informação, fraudes, acessos não autorizados e vazamento de dados.
  - ⇒ O processo deve respeitar princípios éticos, privacidade de dados e normas regulatórias aplicáveis.

- Itens Monitorados:

O monitoramento abrangerá, mas não se limitará a:

  - ⇒ Acessos a sistemas e redes (logs de autenticação e tentativas de login).
  - ⇒ Uso de dispositivos corporativos (incluindo softwares instalados e atividades executadas).
  - ⇒ Tráfego de rede (análise de acessos, tentativas de intrusão e fluxos de dados).
  - ⇒ Transações de dados (transferência de arquivos internos e externos).
  - ⇒ Uso de e-mail e comunicação corporativa (envio e recebimento de mensagens para prevenir vazamento de dados).
  - ⇒ Acesso remoto e conexões externas (VPNs e acessos externos aos ativos institucionais).

- Responsabilidades:
  - ⇒ Equipe de Segurança da Informação (TI): Implementar, configurar e gerenciar as ferramentas de monitoramento, além de analisar e relatar incidentes.
  - ⇒ Gestores de TI e Segurança: Supervisionar as atividades de monitoramento e garantir conformidade com a política.
  - ⇒ Colaboradores e Usuários: Utilizar os recursos computacionais de acordo com as diretrizes estabelecidas e relatar qualquer atividade suspeita.

6.8.3. MONITORAMENTO E EXPECTATIVA DE PRIVACIDADE

- O uso de ativos e serviços institucionais não possui expectativa de privacidade, podendo ser monitorado a qualquer momento.
- Toda atividade realizada nos dispositivos e redes da organização poderá ser registrada, analisada e auditada.

- A organização se reserva o direito de interceptar, registrar, copiar e divulgar informações monitoradas para finalidades legais e investigativas.

6.8.4. GESTÃO DE LOGS E AUDITORIA

- Registros de logs serão armazenados por um período mínimo de [X] meses para rastreabilidade e auditoria.
  - ⇒ O acesso aos logs será restrito à equipe de Segurança da Informação e autorizado somente por gestores responsáveis.
  - ⇒ Auditorias periódicas serão realizadas para garantir a integridade e eficácia dos controles de segurança.

6.8.5. VIOLAÇÕES E SANSÇÕES

- Qualquer tentativa de burlar, desativar ou modificar os mecanismos de monitoramento será considerada infração grave.
- Violações às diretrizes desta política poderão resultar em medidas disciplinares, incluindo advertências, suspensão ou desligamento, conforme a gravidade do incidente.
- Caso identificado crime cibernético, a organização poderá acionar autoridades competentes e colaborar com investigações legais.

6.8.6. REVISÃO E ATUALIZAÇÃO

- Esta política será revisada anualmente ou sempre que necessário, considerando mudanças tecnológicas, regulamentares e organizacionais.

6.9. MONITORAMENTO DE ATIVOS E SEGURANÇA DA INFORMAÇÃO

6.9.1. ABRANGENCIA

- Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros que utilizam os seguintes recursos institucionais:
  - ⇒ Dispositivos computacionais (desktops, notebooks, tablets e smartphones).
  - ⇒ Armazenamento removível (pendrives, HDs externos, cartões de memória e similares).
  - ⇒ Identificação digital (biometria, crachás e tokens de autenticação).
  - ⇒ Equipamentos de impressão e reprografia (impressoras, scanners e copiadoras).
  - ⇒ Conectividade sem fio (Bluetooth, Wi-Fi e NFC).

6.9.2. USO DE ATIVOS COMPUTACIONAIS

- Ativos institucionais devem ser utilizados exclusivamente para atividades profissionais.

- É proibida a instalação de softwares não autorizados e qualquer modificação no hardware sem aprovação da equipe de TI.
- A configuração e o gerenciamento dos dispositivos devem ser realizados somente por profissionais autorizados (TI).
- Equipamentos devem estar sempre protegidos com credenciais seguras, bloqueio de tela e criptografia quando aplicável.

6.9.3. USO DE DISPOSITIVOS DE ARMAZENAMENTO REMOVIVEL (PENDRIVES, HDS EXTERNOS, CARTÕS DE MEMORIA)

- O uso de dispositivos de armazenamento removível é restrito e deve ser autorizado pela equipe de TI.
- Todos os dispositivos removíveis devem ser escaneados por soluções de segurança antes do uso em equipamentos institucionais.
- É proibida a cópia ou armazenamento de informações confidenciais em dispositivos removíveis sem criptografia e autorização prévia.
- O compartilhamento de dispositivos de armazenamento removível entre diferentes sistemas deve ser evitado para reduzir o risco de contaminação por códigos maliciosos.

6.9.4. IDENTIFICAÇÃO DIGITAL E ACESSOS

- Todos os acessos a sistemas, redes e equipamentos devem ser feitos por meio de credenciais individuais e intransferíveis.
- É proibido compartilhar senhas, tokens, crachás ou dispositivos de autenticação com terceiros.
- Sistemas críticos devem exigir autenticação multifator (MFA) para aumentar a segurança dos acessos.
- A identificação biométrica deve ser utilizada sempre que disponível, garantindo maior controle de acessos físicos e digitais.
- Tentativas de burlar mecanismos de autenticação serão consideradas infração grave e sujeitas a sanções disciplinares.

6.9.5. USO DE EQUIPAMENTOS DE IMPRESSÃO E REPROGRAFIA

- O uso de impressoras, scanners e copiadoras deve ser estritamente profissional e justificado.
- Impressões e cópias de documentos confidenciais ou sigilosos devem ser supervisionadas e retiradas imediatamente pelo usuário.

- É proibida a impressão, cópia ou digitalização de documentos pessoais não relacionados às atividades profissionais.
- Todas as impressões e cópias podem ser monitoradas para auditoria e segurança da informação.
- Equipamentos de impressão e reprografia devem ser desligados ou bloqueados quando não estiverem em uso para evitar acessos indevidos.

6.9.6. USO DE CONECTIVIDADE SEM FIO (WIFI E BLUETOOTH)

- O uso de redes Wi-Fi públicas ou não seguras para acessar sistemas corporativos é proibido.
- Para conexões externas, deve-se utilizar VPNs corporativas para garantir a segurança dos dados.
- A conexão Bluetooth deve ser desativada quando não estiver em uso para evitar acessos não autorizados.
- Dispositivos Bluetooth devem estar configurados como não descobertos para evitar tentativas de conexão indevidas.

6.9.7. USO DE WHATSAPP WEB

- Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros que utilizam dispositivos institucionais e acessam a rede corporativa da organização.
- Uso Permitido Somente com Autorização Formal
- O uso do WhatsApp Web será bloqueado por padrão em todos os dispositivos institucionais e redes corporativas.
- O acesso só será permitido mediante solicitação formal, com justificativa da necessidade de uso, e autorização expressa do Gestor de TI e da Segurança da Informação.
- O pedido de acesso deve ser aprovado caso haja justificativa válida, alinhada às atividades profissionais, e será concedido por tempo determinado.
- O acesso autorizado será monitorado continuamente e poderá ser revogado a qualquer momento caso seja identificado uso inadequado.

Restrições Rigorosas para Prevenção de Vazamento de Dados:

- É terminantemente proibido compartilhar informações confidenciais, documentos internos, dados financeiros ou qualquer outro conteúdo sensível via WhatsApp Web.

- O compartilhamento de arquivos e capturas de tela de sistemas internos da organização é estritamente vedado.
- Caso o WhatsApp Web seja necessário para comunicação institucional, deve-se priorizar o uso de canais internos oficiais e plataformas corporativas seguras.
- Qualquer tentativa de burlar as restrições de acesso será considerada uma infração grave, sujeita a medidas disciplinares.

Condições e Procedimentos para Uso Autorizado

- O acesso será concedido apenas para usuários previamente cadastrados e aprovados pela equipe de TI.
- O uso de WhatsApp Web em dispositivos pessoais conectados à rede corporativa é proibido.
- Todas as sessões de WhatsApp Web devem ser encerradas imediatamente após o uso, sem exceções.
- A funcionalidade “Manter-me Conectado” deve ser desativada, exigindo autenticação sempre que for necessário o acesso.

Monitoramento e Auditoria

- O uso do WhatsApp Web será monitorado continuamente para garantir conformidade com as diretrizes de segurança.
- A equipe de Segurança da Informação terá autoridade para revogar acessos concedidos, sem aviso prévio, caso seja detectado qualquer risco ou comportamento suspeito.
- Qualquer violação desta política poderá resultar em sanções disciplinares, incluindo suspensão de acessos e medidas administrativas cabíveis.

6.9.8 - REUNIÕES ONLINE E TELEREUNIÕES INSTITUCIONAIS:

As reuniões online, incluindo aquelas realizadas no âmbito do Projeto Telescope 2 e demais iniciativas institucionais, devem seguir rigorosamente as diretrizes da Política de Segurança da Informação. É obrigatório o uso de plataformas homologadas pela equipe de TI e o acesso deve ocorrer, preferencialmente, por meio de contas corporativas, os participantes devem ser previamente autorizados e identificados.

É vedada a gravação, reprodução ou compartilhamento de conteúdo discutidos sem autorização formal da diretoria responsável. Informações classificadas como confidenciais, estratégicas ou

sensíveis devem ser tratadas com sigilo, e eventuais documentos compartilhados devem estar armazenados em repositórios oficiais e seguros.

Durante as tele reuniões, é de responsabilidade de cada participante assegurar um ambiente físico e digital adequado, evitando exposições indevidas ou escuta por terceiros não autorizados. Dispositivos utilizados devem estar atualizados, protegidos por antivírus e em conformidade com as normas de segurança da instituição.

Qualquer incidente de segurança envolvendo reuniões online deve ser comunicado imediatamente à Gerência de Segurança da Informação. O descumprimento das diretrizes poderá acarretar sanções conforme previsto nesta Política.

6.10. USO DE SOFTWARE LICENCIADO

A organização adota uma política rigorosa de gerenciamento de software, garantindo que apenas softwares licenciados e legalmente adquiridos sejam instalados e utilizados em seus computadores, dispositivos portáteis e servidores. Para assegurar conformidade com a legislação e evitar riscos jurídicos, é proibida a duplicação, reprodução ou distribuição de qualquer software licenciado ou documentação relacionada, salvo quando expressamente autorizado pelo fornecedor ou previsto em contrato de licenciamento. O uso de software não autorizado poderá resultar em sanções administrativas, além de penalidades civis e criminais, conforme estabelecido pela Lei de Direitos Autorais Brasileira.

6.10.1. DIRETRIZES PARA AQUISIÇÃO, USO E GESTÃO DE SOFTWARE

A organização adota uma política rigorosa para a aquisição, instalação, uso e auditoria de software, garantindo conformidade legal e segurança da informação. O uso de qualquer software deve seguir **normas de licenciamento, restrições contratuais e diretrizes internas**, sendo proibida a duplicação ou uso não autorizado.

6.10.2. AQUISIÇÃO E INSTALAÇÃO DE SOFTWARE

- Todo software necessário para atividades profissionais **deve ser adquirido exclusivamente pelo setor de TI**, garantindo licenciamento adequado.
- Apenas **fornecedores autorizados** podem fornecer softwares, incluindo aqueles pré-instalados em hardware adquirido pela organização.

- A instalação de software deve ser realizada **exclusivamente pelo setor de TI**, impedindo que usuários finais instalem programas sem autorização.

6.10.3. USO E RESTRIÇÃO

- Nenhum funcionário pode utilizar software sem uma licença válida adquirida pela organização.
- Antes do uso, os colaboradores devem ser instruídos pelo setor de TI sobre restrições e regras de uso estabelecidas nos contratos de licença.
- O uso de softwares baixados da Internet, incluindo músicas e vídeos protegidos por direitos autorais, é proibido sem a devida permissão do detentor dos direitos.
- Todos os arquivos baixados da Internet devem ser escaneados por um antivírus corporativo antes de sua instalação ou execução.

6.10.4. USO DE SOFTWARE EM COMPUTADORES PESSOAIS

- Computadores institucionais são ativos da organização e só podem conter software legalmente adquirido pela empresa.
- É proibido trazer softwares pessoais e instalá-los nos computadores corporativos.
- Softwares adquiridos pela organização não podem ser instalados em computadores pessoais dos colaboradores.
- Caso haja necessidade do uso doméstico de um software licenciado, o setor de TI verificará se a licença permite essa prática ou adquirirá uma licença adicional.

6.10.5. USO DE SHAREWARE E SOFTWARE LIVRES

- O uso de software shareware está condicionado ao pagamento das taxas exigidas pelo desenvolvedor e ao cumprimento dos termos de licenciamento.
- O setor de TI deve avaliar e aprovar qualquer software shareware antes de sua utilização.

6.10.6. REMOÇÃO DE SOFTWARE

- A remoção de softwares só pode ser feita pelo setor de TI, sendo proibido que usuários excluam ou modifiquem programas instalados.

6.11. CLASSIFICAÇÃO DA INFORMAÇÃO:

- Para efeitos de classificação da informação, o Hospital Nossa Senhora das Dores utiliza as seguintes categorias:
  - ⇒ **INFORMAÇÃO PÚBLICA:** Informação oficialmente liberada pelo Hospital Nossa Senhora das Dores para o público geral. A divulgação deste tipo de informação não causa problemas ao Hospital ou a seus clientes, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.
  - ⇒ **INFORMAÇÃO DE USO INTERNO:** Informação liberada exclusivamente para usuários e departamentos específicos do Hospital Nossa Senhora das Dores, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização expressa.
  - ⇒ **INFORMAÇÃO CONFIDENCIAL:** Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais no Hospital Nossa Senhora das Dores. A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para ao Hospital e/ou seus clientes, portanto seu compartilhamento deve ser restrito e feito de maneira controlada.
- A classificação da informação deverá ser realizada pelos gestores da informação, ou colaboradores designados por estes. Entretanto, a responsabilidade pela assertividade do nível selecionado permanece com o gestor da informação;
- Para informações classificadas como **PÚBLICAS**, poderá ser utilizada um rótulo simples, conforme modelos exibidos no Anexo I desta norma, a critério do setor, podendo optar por não classifica-lo;
- Para informações classificadas como **USO INTERNO** ou **CONFIDENCIAIS,** deverá constar no rótulo a sua classificação e, quanto o acesso à informação for limitado a um setor/departamento específico, o mesmo deverá ser referenciado, conforme modelos exibidos no **Anexo II** desta norma;
- Para a rotulagem da informação, devem ser observados os modelos contidos no **Anexo II** desta norma.

6.11.1. MANUSEIO DA INFORMAÇÃO

- O manuseio da informação do Hospital Nossa Senhora das Dores deverá obedecer às regras definidas na **Tabela Ação x Classificação**, detalhada no **Anexo III** desta norma;
- Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas;
- Em períodos de ausência da estação de trabalho, documentos em suporte físico devem ser retirados das mesas e de outras áreas de superfície;
- Documentos de uso interno ou confidenciais em suporte eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas;
- Toda não-conformidade será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

6.11.2. DESCARTE DA INFORMAÇÃO

- O descarte da informação deve ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original;
- O descarte da informação deverá ser realizado conforme os métodos estabelecidos no **Anexo IV** desta norma.

Documentos confidenciais em suporte físico devem ser guardados em gavetas ou armários trancados.

7. RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

O Plano de Resposta a Incidentes de Segurança da Informação do HNSD define diretrizes para identificar, comunicar, conter e tratar eventos que comprometam a confidencialidade, integridade ou disponibilidade das informações institucionais. Estabelece a atuação do Time de Resposta a Incidentes (TRI), composto por áreas-chave como TI, Jurídico, Comunicação e Privacidade. Os incidentes são classificados e priorizados conforme o impacto e a criticidade. Em casos de vazamento de dados, a notificação à ANPD será avaliada em até 48 horas. Após a contenção, realiza-se uma análise de causa raiz e ações corretivas. O sigilo das informações é obrigatório. O não cumprimento das diretrizes está sujeito a sanções administrativas e legais. O plano é revisado periodicamente pelo Comitê de Segurança da Informação. Conforme PRS-CI-002-RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO.

8. SANSÕES E PUNIÇÕES

8.1. As violações, mesmo que por mera omissão ou tentativa não consumada desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

8.2. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

8.3. No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

8.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 7.1, 7.2 e 7.3 desta política.

9. BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBRISO/IEC27001, Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos, mar. de 2006.

LAUREANO, Marcos Aurélio Pchek - UMA ABORDAGEM PARA A PROTEÇÃO DEDETECTORES DE INTRUSÃO BASEADA EM MÁQUINAS VIRTUAIS. Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática Aplicada, 2004.

LAUREANO, Marcos Aurélio Pchek – GESTÃO DE SEGURANÇA DA INFORMAÇÃO. Arquivo baixado dia 07 de julho de 2011, do site: http://www.mlaureano.org/ensino/gestao-da-seguranca/.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000.

10. ANEXOS

ANEXO I – TERMO DE USO DE SISTEMAS INTERNOS

CONSIDERANDO que o Hospital Nossa Senhora das Dores-HNSD e Pronto Socorro Municipal de Itabira-PSMI disponibiliza a seus usuários ativos de informação e recursos computacionais exclusivamente para que eles possam desempenhar suas atividades profissionais;

CONSIDERANDO que o Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira é o único proprietário de todos os ativos de informação e recursos computacionais, dessa forma, sendo responsável por todos os custos com os mesmos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

CONSIDERANDO que o Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira poderá ser seriamente impactado pela má utilização de seus ativos de informação e recursos computacionais;

DECLARO QUE:

1. Tenho conhecimento e acesso a Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, que se encontram disponíveis na unidade de rede **Pol Seg Informação (v:)**, bem como ao canal de denúncia (https://app.protegon.com.br/#/external_incident_complaint/78bdbe73), canal de Termos de Uso e Política de Privacidade (https://app.protegon.com.br/#/external_request/27f9a597), aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;
2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;

3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira somente poderá ser utilizada para fins exclusivamente profissionais e relacionados às atividades da organização;

4. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica do Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira;

5. Estou ciente que violações da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;

6. Comprometo-me a não revelar, fato ou informações de qualquer natureza a que tenha conhecimento por forças das minhas atribuições, mesmo após o encerramento do contrato de trabalho com Hospital Nossa Senhora das Dores e Pronto Socorro Municipal de Itabira.

Itabira, _____ de _____ de 20___.

ANEXO **II – MODELOS PARA ROTULAGEM DE INFORMAÇÕES**

Os padrões a seguir representam os rótulos aprovados que devem ser exibidos nos cabeçalhos e rodapés de documentos de acordo com seu nível de classificação.

Observação: A cor, fonte e tamanho do texto podem ser ajustados para adequação a informação rotulada, desde que mantida a clareza e objetividade da informação

1.1. Cabeçalho

Nível	Rótulo
Informação Pública (Rotulagem opcional)	PÚBLICO *Informação Pública* *Public Information*
Informação Interna	INTERNO *Informação Interna* *Internal Information*
Informação Confidencial	CONFIDENCIAL *Informação Confidencial* *Confidential Information*

Tabela 1. Cabeçalho.

1.2. Rodapé

<RAZÃO SOCIAL DA EMPRESA> – [INSERIR NÍVEL DE CLASSIFICAÇÃO/SETOR]

Exemplo:

HOSPITAL NOSSA SENHORA DAS DORES – Uso Interno / Departamento de Recursos Humanos

---

ANEXO III – MODELOS PARA ROTULAGEM DE INFORMAÇÕES

Os padrões a seguir representam os rótulos aprovados que devem ser exibidos nos cabeçalhos e rodapés de documentos de acordo com seu nível de classificação.

Observação: A cor, fonte e tamanho do texto podem ser ajustados para adequação a informação rotulada, desde que mantida a clareza e objetividade da informação

1.1. Cabeçalho

Nível	Rótulo
Informação Pública (Rotulagem opcional)	PÚBLICO *Informação Pública* *Public Information*
Informação Interna	INTERNO *Informação Interna* *Internal Information*
Informação Confidencial	CONFIDENCIAL *Informação Confidencial* *Confidential Information*

Tabela 1. Cabeçalho.

1.2. Rodapé

<RAZÃO SOCIAL DA EMPRESA> – [INSERIR NÍVEL DE CLASSIFICAÇÃO/SETOR]

Exemplo:

HOSPITAL NOSSA SENHORA DAS DORES – Uso Interno / Departamento de Recursos Humanos

---

ANEXO IV – TABELA AÇÃO X CLASSIFICAÇÃO

AÇÃO	CLASSIFICAÇÃO		
	Pública	Interna	Restrita / Confidencial
Cópia / Exclusão	Sem restrições	Sem restrições	Permissão do gestor da informação
Envio por e-mail	Sem restrições	Usar texto destaque padronizado	Usar texto destaque padronizado
Transmissão em rede pública	Permitido	Permitido	Recomendável comunicação criptografada.
Descarte	Lixo comum	Lixo comum. Recomendável uso de fragmentadora.	Utilizar métodos aprovados conforme anexo desta norma.
Envio a terceiros	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação e termo de confidencialidade assinado pelo terceiro.
Solicitação de direitos de acesso	Sem restrições	Aprovação do gestor da informação	Aprovação do gestor da informação
Correio interno e externo	Envelope comum	Envelope comum	Envio para destinatário específico identificado apenas dentro do envelope.
Rotulagem	Opcional	Na capa e em todas as páginas	Na capa e em todas as páginas.
Registro de Acompanhamento	Opcional	Opcional	Destinatários, cópias efetuadas, localização e endereço de todos que acessaram e destruição.

ANEXO V – MÉTODOS DE DESCARTE PARA INFORMAÇÕES ARMAZENADAS

Os métodos a seguir foram selecionados como forma segura de garantir o descarte de informações do Hospital Nossa Senhora das Dores.

Para todos os métodos que envolvem atividades técnicas, os usuários deverão encaminhar a solicitação para a área de tecnologia da informação.

Método	Descrição	Aplicável a
Sobre gravar mídia	Sobre gravar dados em mídias de armazenamento magnético com informações não sensíveis por pelo menos 07 vezes. Essa tarefa pode ser executada com o auxílio de software/hardware especializado. Este método não destrói fisicamente a mídia, entretanto destrói todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis, CDR, DVDR e similares;
Destruição física	Destruição física da mídia de armazenamento com o uso de fragmentadora especializada, pulverizadores ou incineradores. Este método destrói completamente a mídia e todos os dados.	Discos rígidos, disquetes, fitas, flash disks, discos removíveis. CD, CDR, DVD, DVDR. Este método também é válido para material em suporte físico como impressos e similares;
Desmagnetização	Desmagnetização de mídias como fitas e disquetes. Este método destrói todos os dados.	Fitas e disquetes.

Controle De Revisão			
Revisão	**Data**	**Item**	**Natureza das Alterações**
0	15/05/2025	Sumário	Padronização correta do Sumário.
1	02/06/2025	7. Resposta a Incidente da Informação	Foi incluído o item 7. Vinculado ao PRS-CI-002

Controle Histórico				
Revisão	**Data**	**Elaboração**	**Verificação**	**Aprovação**
0	15/05/2025	Leandro Alencar	Deyvison Roberto	Welisson Reis
1	02/06/2025	Leandro Alencar	Deyvison Roberto	Welisson Reis